UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/595,016	05/10/2006	Vesa Torvinen	P18450US1	1254

27045 7590 01/17/2008

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
BENOIT, ESTHER	

ART UNIT	PAPER NUMBER
4152	

MAIL DATE	DELIVERY MODE
01/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/595,016	TORVINEN ET AL.	
	Examiner	Art Unit	
	ESTHER BENOIT	4152	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/16/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20, and 22-32 are pending in this application. Claims 2-7 are amended and claims 18-20, and 22-32 are added by a preliminary amendment filed on 12/16/2005.

Specification

2. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code which can be found on page 2, line 5 of the disclosure.

Claim Objections

3. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Misnumbered claims 22-32 have been renumbered to 21-31.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 2, and 4 are rejected under 35 U.S.C. 102(b) as being anticipated by Franks et al. (RFC 2069- An Extension to HTTP: Digest Access Authentication)

With respect to claim 1, Franks discloses a method of generating a password for use by an end-user device (UE) to access a remote server, comprising: sending a request for access from the UE to the remote server; (pg. 4, paragraph 7, "Where client-IP…", lines 1-2) creating a temporary identity for the UE; (pg. 4, paragraph 5, "A server-specified..", lines 1-2) sending to an authentication node in the UE's home network details of the request for access; (pg. 4, paragraph 7, lines 3-6) at the authentication node or the remote server, generating a Hypertext Transfer Protocol (HTTP) Digest challenge using an algorithm capable of generating end-user passwords, including details of the temporary identity of the UE; (pg. 5, paragraph 4, "A string indicating…", lines 3-5) at the UE, generating a password based on the HTTP Digest challenge, said password being associated with the identity of the remote server and the

identity of the UE; (pg. 4, paragraph 5, "A server-specified..", lines 1-2) and storing the password and the temporary identity of the UE at the UE (pg. 12, paragraph 7, "Digest Authentication..", lines 1-3)

With respect to claim 2, Franks discloses the method, wherein the algorithm capable of generating end-user passwords is HTTP Digest Authentication and Key Agreement (AKA) (pg. 5, paragraph 4, "A string indicating...", lines 3-5)

With respect to claim 4, Franks discloses the method, wherein the temporary identity of the UE is created at the remote server (pg. 4, paragraph 5, "A sever-specified…", lines 1-2)

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 3, and 15-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franks et al. (RFC 2069- An Extension to HTTP: Digest

Access Authentication) as applied to Claim 1 above, in view of Niemi et al. (RFC, HTTP Digest Authentication Using AKA)

With respect to claim 3, Franks does not disclose the method, further comprising sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server, and wherein the identity of the remote server is stored at the UE. However, Niemi discloses sending the identity of the remote server to the authentication node, (pg. 7, paragraph 2, "A parameter which...", lines 1-3) wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server, (pg. 7, paragraph 2, "A parameter which...", lines 1-3) and wherein the identity of the remote server is stored at the UE (pg. 3, paragraph 2, "The authentication..", lines 4-7)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks with the teachings of Niemi to use the identity of the remote server stored on the end user to generate the HTTP Digest Challenge, in order to know which remote server the client is communicating with.

With respect to claim 15, Franks discloses a method of accessing a remote server from an end-user device (UE), the method comprising: generating and storing a password; sending a request for access from the UE to the remote

server; (pg. 4, paragraph 7, "Where client-IP…", lines 1-2) at the remote server, generating a Hypertext Transfer Protocol (HTTP) Digest challenge including details of the identity of the remote server and sending the challenge to the UE; (pg. 5, paragraph 4, "A string indicating…", lines 3-5). Franks does not disclose sending an authentication response including the temporary identity of the UE and a proof of possession of the password to the remote server. However, Niemi discloses sending an authentication response including the temporary identity of the UE and a proof of possession of the password to the remote server (pg. 5, paragraph 5, "Using the shared..", lines 2-5 and paragraph 6, "The authentication response..")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks with the teachings of Niemi to send an authentication response to the remote server in order to verify if the client has been authenticated or not.

With respect to claim 16, Franks does not disclose the method, further comprising sending an authentication request from the remote server to the authentication node, sending the password from the authentication node to the remote server, and authenticating the UE at the remote server. However, Niemi discloses sending an authentication request from the remote server to the authentication node, (pg. 5, paragraph 3, "The server creates..") sending the password from the authentication node to the remote server, (pg. 5, paragraph

5, "Using the shared secret..", lines 2-5; paragraph 6, "The authentication response..") and authenticating the UE at the remote server (pg. 7, paragraph 4, "If the serer receives..", lines 1-2)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks with the teachings of Niemi, in order to securely authenticate the client at the remote server.

With respect to claim 17, Franks does not disclose the method, further comprising sending an authentication request from the remote server to the authentication node, authenticating the UE at the authentication node, and sending confirmation of authentication from the authentication node to the remote server. However, Niemi discloses sending an authentication request from the remote server to the authentication node, (pg. 5, paragraph 3, "The server creates..") authenticating the UE at the authentication node, (pg. 5, paragraph 5, "Using the shared..", lines 2-5) and sending confirmation of authentication from the authentication node to the remote server (pg. 5, paragraph 6, "The authentication response..")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks with the teachings of Niemi to send confirmation of authentication from the authentication

node to the remote server, in order to verify if the client has been authenticated or not.

With respect to claim 18, Franks discloses the method, wherein the step of generating and storing a password further comprises: creating a temporary identity for the UE; pg. 4, paragraph 5, "A server-specified..", lines 1-2) sending to an authentication node in the UE's home network details of the request for access; (pg. 4, paragraph 7, lines 3-6) at the authentication node, generating a Hypertext Transfer Protocol (HTTP) Digest challenge using an algorithm capable of generating end-user passwords including details of the temporary identity of the UE; (pg. 5, paragraph 4, "A string indicating...", lines 3-5) at the UE, generating a password based on the HTTP Digest challenge, said password being associated with the identity of the remote server and the identity of the UE; (pg. 4, paragraph 5, "A server-specified..", lines 1-2) and storing the password and the temporary identity of the UE at the UE (pg. 12, paragraph 7, "Digest Authentication..", lines 1-3)

With respect to claim 19, Franks discloses the method, wherein the algorithm capable of generating end-user passwords is HTTP Digest Authentication and Key Agreement (AKA) (pg. 5, paragraph 4, "A string indicating...", lines 3-5)

With respect to claim 20, Franks does not disclose the method, further comprising sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server, and wherein the identity of the remote server is stored at the UE. However, Niemi discloses sending the identity of the remote server to the authentication node, (pg. 7, paragraph 2, "A parameter which…", lines 1-3) wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server, (pg. 7, paragraph 2, "A parameter which…", lines 1-3) and wherein the identity of the remote server is stored at the UE (pg. 3, paragraph 2, "The authentication..", lines 4-7)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks with the teachings of Niemi to use the identity of the remote server stored on the end user to generate the HTTP Digest Challenge, in order to know which remote server the client is communicating with.

With respect to claim 21, Franks discloses the method, wherein the temporary identity of the UE is created at the remote server (pg. 4, paragraph 5, "A sever-specified…", lines 1-2)

8. Claims 5-9, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franks et al. (RFC 2069- An Extension to HTTP: Digest Access Authentication) as applied to Claim 1 above, in view of Kadyk et al. (US 6,996, 841 B2)

With respect to claim 5, Franks does not disclose the method, wherein the step of sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node. However, Kadyk discloses sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node (Col. 13, lines 16-20)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks with the teachings of Kadyk to include redirecting the request for access to the authentication node if the client is being authenticated at the authentication node.

With respect to claim 6, the claim is rejected for the same reason as Claim 5 above. In addition, Kadyk discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE (Col. 11, lines 53-55)

With respect to claim 7, Franks discloses the method, wherein the password is stored at the authentication node (pg. 8, paragraph 4, "Upon receiving...", lines 1-3)

With respect to claim 8, the claim is rejected for the same reason as Claim 5 above. In addition, Kadyk discloses authenticating the UE at the authentication node and redirecting the request for access from the authentication node to the remote server after the password has been generated (Col. 12, lines 6-8)

With respect to claim 9, Franks does not disclose the method, wherein the step of sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly,. However, Kadyk discloses sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly (Col. 13, lines 16-20)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks with the teachings of Kadyk to have the remote server contact the authentication node directly since the password is stored at the authentication node. This allows a more appropriate way for the remote server to contact the authentication node directly and authenticate the client.

With respect to claim 11, Franks discloses the method, wherein the HTTP Digest challenge is generated at the remote server (pg. 4, paragraph 5, "A server-specified...", lines 1-2)

9. Claims 10, and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franks et al. (RFC 2069- An Extension to HTTP: Digest Access Authentication) as applied to Claims 9 and 15 above, in view of Kadyk et al. (US 6,996, 841 B2), and further in view of Niemi et al. (RFC, HTTP Digest Authentication Using AKA)

With respect to claim 10, Franks and Kadyk do not disclose the method, wherein the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the remote server. However, Niemi discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the remote server (pg. 7, paragraph 4, "If the server..", lines 1-4)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks and Kadyk with the teachings of Niemi to generate the HTTP Digest Challenge at the authentication node and send it from the authentication node to the remote server, in order to authenticate the client at the remote server.

With respect to claim 12, the claim is rejected for the same reason as Claim 10 above. In addition, Niemi discloses the method, further comprising sending the HTTP digest challenge from the remote server to the UE (pg. 7, paragraph 5, "When a client...", line 1)

With respect to claim 13, Franks and Kadyk do not disclose the method, further comprising including a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server. However, Niemi discloses a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server (pg. 7, paragraph 5, "When a client.."; pg. 8, paragraph 1, "The AUTN token..")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks and Kadyk with the teachings of Niemi to send the HTTP Digest AKA challenge password from the authentication node to the remote server and then authenticate the user at the remote server, in order to use a more secure password to authenticate the user at the remote server.

With respect to claim 14, Franks and Kadyk do not disclose the method, further comprising authenticating the UE at the authentication node and returning an authentication result to the remote server. However, Niemi

discloses authenticating the UE at the authentication node and returning an authentication result to the remote server (pg. 5, paragraph 5, "Using the shared secret..", lines 2-5; paragraph 6, "The authentication response")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks and Kadyk with the teachings of Niemi to return an authentication result to the remote server, in order verify if the client has been authenticated or not.

10. Claims 22-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franks et al. (RFC 2069- An Extension to HTTP: Digest Access Authentication) as applied to Claims 1 and 15 above, in view of Niemi et al. (RFC, HTTP Digest Authentication Using AKA), and further in view of Kadyk et al. (US 6,996, 841 B2)

With respect to claim 22, Franks and Niemi do not disclose the method, wherein the step of sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node. However, Kadyk discloses sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node (Col. 13, lines 16-20)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks and Niemi with the teachings of Kadyk to include redirecting the request for access to the authentication node if the client is being authenticated at the authentication node.

With respect to claim 23, the claim is rejected for the same reason as Claim 22 above. In addition, Kadyk discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE (Col. 11, lines 53-55)

With respect to claim 24, Franks discloses the method, wherein the password is stored at the authentication node (pg. 8, paragraph 4, "Upon receiving...", lines 1-3)

With respect to claim 25, the claim is rejected for the same reason as Claim 22 above. In addition, Kadyk discloses authenticating the UE at the authentication node and redirecting the request for access from the authentication node to the remote server after the password has been generated (Col. 12, lines 6-8)

With respect to claim 26, Franks and Niemi do not disclose the method, wherein the step of sending details of the request for access to the authentication node includes the remote server contacting the authentication

node directly. However, Kadyk discloses sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly (Col. 13, lines 16-20)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks and Niemi with the teachings of Kadyk to have the remote server contact the authentication node directly since the password is stored at the authentication node. This allows a more appropriate way for the remote server to contact the authentication node directly and authenticate the client.

With respect to claim 27, Franks does not disclose the method, wherein the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the remote server. However, Niemi discloses the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the remote server (pg. 7, paragraph 4, "If the server..", lines 1-4)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks with the teachings of Niemi to generate the HTTP Digest Challenge at the authentication node and send it from the authentication node to the remote server, in order to authenticate the client at the remote server.

With respect to claim 28, Franks discloses the method, wherein the HTTP Digest challenge is generated at the remote server (pg. 4, paragraph 5, "A server-specified...", lines 1-2)

With respect to claim 29, the claim is rejected for the same reason as Claim 27 above. In addition, Niemi discloses the method, further comprising sending the HTTP digest challenge from the remote server to the UE (pg. 7, paragraph 5, "When a client...", line 1)

With respect to claim 30, Franks does not disclose the method, further comprising including a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server. However, Niemi discloses a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server (pg. 7, paragraph 5, "When a client.."; pg. 8, paragraph 1, "The AUTN token..")

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Franks with the teachings of Niemi send the HTTP Digest AKA challenge password from the authentication node to the remote server and then authenticate the user at the remote server, in order to use a more secure password to authenticate the user at the remote server.

With respect to claim 31, the claim is rejected for the same reason as Claim 27 above. In addition, Niemi discloses authenticating the UE at the authentication node and returning an authentication result to the remote server (pg. 5, paragraph 5, "Using the shared secret..", lines 2-5; paragraph 6, "The authentication response")

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esther Benoit whose telephone number is 571-270-3807. The examiner can normally be reached on Monday through Friday between 7:30 a.m and 5 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nabil El-Hady can be reached on 571-272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

E.B.
Dec. 27, 2007

/Nabil El-Hady, Ph.D, M.B.A./
Supervisory Patent Examiner, Art Unit 4152